PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology
Service Delivery & Engineering

Region 1 Pager Services Consolidation

Date: 01/12/2015

TAC-15-18232
ITARS 597364

PWS Version Number: 2.0

Contents

DRAFT

DRAFT

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Veterans Health Administration (VHA), Office of Information & Technology (OI&T), is to support the provision of benefits and services to Veterans of the United States. In meeting these goals, OI&T strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' healthcare systems in an effective, timely, and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

OI&T Region 1 Telecommunications Business Office (TBO) is responsible for providing pager devices and related pager services to Department of Veterans Affairs Medical Centers (VAMC) and responsible outliers throughout Region 1, Veterans Integrated Service Networks (VISN) 18, 19, 20, 21 and 22. These pager services are critical to VA's mission and directly impact VA's ability to provide quality care to our Veterans. The VA depends upon External Paging services to meet its goals, and responsibilities of providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' healthcare systems in an effective, timely, and compassionate manner.

VA requires external paging services for the VAMC and responsible outliers throughout Region 1, VISNs 18, 19, 20, 21, and 22. In addition, the VA requires one way, two way external paging devices and accessories as part of the paging services. These services shall be offered on a local or statewide, regional, and national basis using the Contractors digital networks exclusively provisioned and dedicated to critical messaging paging services on the contractor's network.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"

7. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
8. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” May 18, 2007
9. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
10. Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” November 28, 2000
11. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
12. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
13. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
14. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, , 2012
15. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
16. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
17. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
18. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
19. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
20. VA Handbook 6500.6, “Contract Security,” March 12, 2010
21. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at https://www.voa.va.gov/)
22. OI&T ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at https://www.voa.va.gov/) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
23. Technical Reference Model (TRM) (reference at https://www.voa.va.gov/)
24. National Institute Standards and Technology (NIST) Special Publications (SP)
25. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
26. VA Directive 6300, Records and Information Management, February 26, 2009
27. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010

3.0 SCOPE OF WORK

The Contractor shall provide pager types, features and plans for external paging services to meet the needs of VA Region 1 described herein. The Contractor’s external leased paging services shall include VA personnel access to a web-based portal for moves, adds, and changes. The Contractor shall also provide training, maintenance,

and shipping and return support. In addition, the Contractor shall support the maintenance and the installation and/or removal of two-way external local pager consoles and/or transmitters and related equipment at VHA Region 1 locations.

The Contractor must be able to provide external analog or digital pagers and services as compared to what is currently used at facilities. Under no circumstances should any VA Medical Center or its pager users be without service. Contractor must ensure that at no time the VA will be without emergency contact in the event of a paging system outage or outage of automated exchanging system. Contractor must have a backup arrangement or system in place for any interruption of service due to Contractor system problems, outages, maintenance, hardware or software upgrades or changes. There will be no change of services unless the Government requests a change. The Government is not responsible for purchasing any new equipment to accommodate vendor services due to any vendor inability to provide coverage, to include installation of antennae, etc. There shall be no down time for installation or cut-over at any facility covered under this contract. The Government requires the ability to have United States Homeland Security Telecommunications Priority Service (TPS) Restoration program.

4.0 PERFORMANCE DETAILS

4.1 CONTRACT TYPE

This is a Firm-Fixed-Price (FFP) contract.

4.2 PERFORMANCE PERIOD

The performance period shall be a 6-month base period starting April 01, 2015 through September 30, 2015, with two, 12-month option periods.

Any work at a Government sites shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO). If required, the CO may designate the Contractor to work during holidays and weekends.

There is ten Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.3 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed remotely at Contractor facilities.

4.4 TRAVEL

There is no travel anticipated for performance of the tasks in this effort.

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 MEETING REQUIREMENTS

For successful management and contract surveillance, the following reviews are required.

5.1.1 PROGRAM PROGRESS REVIEWS

The Contractor shall conduct Program Progress Reviews (PPR) for Government personnel at a mutually agreeable facility (meeting can be virtual). The COR will schedule the initial PPR. It is anticipated the first PPR will occur no later than 90 calendar days after date of contract award. Thereafter, PPRs shall occur quarterly, for the life of the contract. During each PPR, the Contractor shall present material that addresses:

1. Status of current services
2. Activities determined to be of importance to VA, such as unanticipated problems
3. Status of significant issues
4. How issues are to be resolved by VA or Contractor

The Contracting Officer Representative (COR) shall produce and distribute the PPR meeting minutes identifying the key discussion points and action items. The COR shall deliver the PPR meeting minutes to the COR within five business days after the PPR.

5.2 PROJECT MANAGEMENT

5.2.1 REPORTING REQUIREMENTS

All reports will be accessed by VA employees as needed via the web-portal as specified in Section 5.7.

Examples of report types needed are:

a. Units in service, by type, billed customer, department.
b. Calls, by billed customer, pager number, department
c. Overcalls by billed customer, pager number, department
d. New sales, charges, or disconnects
e. Account Summary by sub-accounts
f. Zero-use devices

5.3 PAGER LEASING

The Contractor shall provide one way, two-way paging messaging services, and wireless information services throughout the Continental United States and its territories to include Alaska, Hawaii, and Puerto Rico. These services shall be offered on a local or statewide, regional, and national basis using digital networks exclusively provisioned and dedicated to critical messaging paging services on the contractor's network. The contractor shall include the pager devices as part of the paging services. The number of numeric and alphanumeric pagers and services throughout the Period of Performance (PoP) is expected to remain relatively static. VA anticipates a deviation of no more than +/- 10% of the total numbers and types of these pagers in each option year from the prior year, due to the fluidity of employee numbers and needs. However, proclivity for two-way paging is on the rise and waiting area paging is seeing relative increase due to customer service initiatives. It is anticipated that the need for these pagers may increase by 10% per year.

The Contractor's standard commercial warranty shall apply to furnished or installed equipment.

All pagers shall include basic paging service. The Government anticipates ten percent of the pagers may have one additional feature or services, an additional ten percent may have two additional features or services and a small portion may have three or more services. Additional paging services are detailed in the table below.

Additional Paging Services	
CODE Pagers	Group Paging Setup
Emergency Notification	Operator Dispatch
Message Carbon Copy	Custom Greeting
Alias Email	Page Saver
Additional Number	Page Forwarding
Toll Free Number	Numeric Retrieval
Secondary Toll-Free Number	Voice Mail Option 1; 15 Msg, 72 hrs, 60 sec
Group Call Lead/Follow	Voice Mail Option 2; 10 Msg, 24 hrs, 45 sec
Short Message Service (SMS)	Voice Mail Option 3 10 Msg, 12 hrs, 30

	sec
Two-Way Group Call Feature	Dispatch Software

Table 1: Additional Paging Services

5.3.1 BASE YEAR PAGER LEASES

The Contractor shall lease up to the number/type of pagers specified below:

BASE YEAR PAGERS (Not to Exceed (NTE) Quantities)		
Pager Type	**Pager Class**	**Subtotals**
Numeric (6500)	Local	Up to 6500
	Regional/State	Up to 50
	National	Up to 50
Alphanumeric (7,500)	Local	Up to 7500
	Regional/State	Up to 120
	National	Up to 120
Two-way	National	Up to 120
Courtesy	National/Local*	Up to 120
	Total	Up to 14,580

Table 2: Base Year Pager Leases

Base Year Pager Quantities

* Local is off net of the national paging network. Nationwide is on the national paging network. Courtesy pagers shall operate at Government allotted frequencies.

Deliverables:

A. Numeric Pagers with unlimited pager services
B. Alphanumeric pagers with unlimited pager services
C. Two Way pagers with unlimited pager services
D. Additional Paging Services

5.3.2 PAGING SERVICE CONTRACT TRANSITION (BASE CONTRACT LEVEL)

The 14,580 pagers identified in the table above are currently in-service/activated under an existing contract that expires on March 31, 2015. In the event of a change in pager service provider, the Contractor shall ensure that all in-service/pager numbers are ported over and there are no service disruptions on day one of the period of performance. In addition, the Contractor shall ensure that the configuration of existing services is maintained (e.g. pager groups, features). The Contractor must port 100% of all original

pager numbers. The Contractor shall identify all current business processes which are dependent on the paging system and have those business processes configured and activated to prevent service disruption as well. Examples of business processes include group paging, reaction team paging and email alerting. The Contractor will provide Code Pagers and the code pagers generally have a computer interface, whereas there is a single login, the VA can set up paging groups via this interface, and receive an acknowledgement of the page. The steps required for sending out a code blue page to the Code Blue Pagers shall be minimized to a point that takes less than 30 seconds to send out the page once logged into the Contractors interface. Logging into the Contractors interface shall consist of a single login action. The Contractor shall document the detailed transition steps in a Paging Services Transition Plan which shall be reviewed and approved by the Government. The Contractor shall provide equal or better service coverage to what is currently provided at each facility. In the event lower than acceptable coverage is provided, the Contractor shall be responsible for any remedy needed to provide adequate coverage including but not limited to the installation of an additional antenna. Service coverage issues must be remediated within 30 days of being identified by the Government.

Deliverables:

A. Paging Services Transition Plan

5.4 PAGER DEVICE ACCESSORIES

5.4.1 BASE 6 Months PAGER ACCESSORIES

The Contractor shall provide the following pager accessories:

BASE YEAR COURTESY PAGER ACCESSORIES (NTE Quantities)	
ACCESSORY	**QUANTITIES**
Cluster Charger	Up to 30*
Replacement AC Adapter for Cluster Charger	Up to 4
Replacement Charger for Single Courtesy Pager Unit.	Up to 33
Replacement Battery for Courtesy Pager	Up to 85

Table 3: Base Year Courtesy Pager Accessories

***** Assumes each cluster charger charges ten (10) courtesy pagers.

BASE 6 Months PAGER ACCESSORIES (NTE Quantities)			
ACCESSORY	NUMERIC PAGER	ALPHANUMERIC PAGER	TWO-WAY PAGER
Replacement Battery Cover	514	65	33
Belt Clips	514	65	33
Harsh Environment Protective Cas-es	514	65	33
Faceplates	514	65	33

Table 4: Base 6 Months Pager Accessories

Deliverable:

A. Cluster Charger(s)
B. Replacement AC Adapter(s) for Cluster Charger
C. Replacement Charger(s) for Single Courtesy Pager Unit
D. Replacement Battery for Courtesy Pager(s)
E. Replacement Battery Cover(s)
F. Belt Clip(s)
G. Harsh Environment Protective Case(s)
H. Faceplate(s)

5.4.2 OPTION PERIOD ONE YEAR PAGER ACCESSORIES

The Contractor shall provide the following pager accessories:

OPTION YEAR ONE COURTESY PAGER ACCESSORIES (NTE Quantities)	
ACCESSORY	QUANTITIES
Cluster Charger	Up to 15
Replacement AC Adapter for Cluster Charger	Up to 2
Replacement Charger for Single Courtesy Pager Unit	Up to 16
Replacement Battery for Courtesy Pager	Up to 16

Table 5: Option Year One Courtesy Pager Accessories

***** Assumes each cluster charger charges ten (10) courtesy pagers.

DRAFT

OPTION PERIOD ONE PAGER ACCESSORIES (NTE Quantities)			
ACCESSORY	**NUMERIC PAGER**	**ALPHANUMERIC PAGER**	**TWO-WAY PAGER**
Replacement Battery Cover	257	33	17
Replacement AC Adapter	257	33	17
Belt Clips	257	33	17
Harsh Environment Protective Cases	257	33	17
Faceplates	257	33	17

Table 6: Option Period One Pager Accessories

Deliverable:

A. Cluster Charger(s)
B. Replacement AC Adapter(s) for Cluster Charger
C. Replacement Charger(s) for Single Courtesy Pager Unit
D. Replacement Battery for Courtesy Pager(s)
E. Replacement Battery Cover(s)
F. Belt Clip(s)
G. Harsh Environment Protective Case(s)
H. Faceplate(s)

5.5 PAGER SERVICE PLANS

The Contractor shall offer the following service plans:

a. Unlimited Calls: Numeric, Alphanumeric
b. Unlimited Characters: Two-Way
c. Pager Synchronicity Services
d. Code Paging services (internet interface to transmit Code Blue Pages)

A detailed list of required service plans is provided in PWS Section 5.3.

The Contractor shall notify the VA COR, or his designate, and the VA National Service Desk (NSD) of any scheduled system outages at least 72 hours (including holiday and weekend hours) in advance of the planned outage. In case of any unforeseen outages, the VA COR and the NSD shall be notified within four hours by both email and telephone call and kept up-to-date on the progress until service restoration. If the unscheduled outage is anticipated to be more than 24 hours, Contractor must provide an alternate plan for service coverage acceptable to VA.

These pager services are critical to VA's mission and directly impact VA's ability to provide quality care to our Veterans. The Contractor shall ensure that all pager service plans provided under this contract are eligible for the United States Homeland Security Telecommunications Service Priority (TSP) Restoration program, under the Wireless Priority Services (WPS). All pager services supplied under this contract must receive

priority treatment under the WPS program. The contractor shall include basic service plans in the cost of the lease for each pager. All VA accounts must be identified in the Contractor's network as a Federal Government account and shall not be disconnected for any reason unless requested by the Government.

5.6 PAGER MANAGEMENT SERVICES

Contractors shall coordinate initial deliveries with Site Point of Contracts (POC) before shipment of hardware to ensure sites are ready to receive the equipment.

All shipments to the Government, either as single or multiple container deliveries shall bear the VA Purchase Order (PO) number on external shipping labels and associated manifests or packing lists. The Contractor shall ensure multiple container deliveries indicate total number of containers for the complete shipment near the VA PO number (e.g., Package 1 of 2), clearly readable on manifests and external shipping labels.

5.6.1 SUBSEQUENT PAGER REPLACEMENT

The Contractor shall support the replacement of any pager types, including the associated features and plans specified in this PWS, under warranty in the event of manufacturer defect or malfunctions not due to neglect or abuse; and, in the event of loss or breakage, provide replacements at the quoted replacement price. Contractor shall also provide for refreshments and upgrades of devices due to normal wear and tear or end-of-life support.

VA acknowledges that pagers are the property of the Contractor and will be returned upon completion of the contract. Pagers that are not returned within 30 days of notice shall be charged to the Government. Each pager service (e.g. numeric, alphanumeric, local, and regional) shall support unlimited pages on a monthly basis. The Contractor shall provide a single contact and contact information, including phone and e-mail, to the VA COR and VA site POCs.

5.6.2 RETURNS SHIPPING SUPPORT

VA anticipates that 5% of pagers will be returned to be repaired or replaced per year. In addition, the Government may return pagers not needed or to maintain a back stock of no more than 3% of spare devices; or, for the purpose of receiving credit for returning unneeded pagers. The Government will return devices via common carrier. The contractor shall propose a device return procedure.

Prior to Contractor shipping devices, the Contractor shall notify Site POCs, by phone or email, of all incoming deliveries including line-by-line details for review of requirements. Only the COR is authorized to make changes to delivery schedules.

Deliverable:

A. Return Shipping Procedure

5.7 WEB-BASED PORTAL FOR BASE AND OPTION PERIOD

5.7.1 SYSTEM CAPABILITIES

The Contractor shall provide a web-based access to VA facility managers for accounts access and management. It shall also enable facility managers to assign, activate, swap, or disconnect devices. The VA COR will provide the Contractor with a list of Government employees who will need access to the web-based portal and the account numbers.

5.7.2 REPORTS

The Contractor shall provide the VA with the capability of running reports through the web-based portal. The number and names of the individuals will be determined at contract award; not to exceed 50 users. R1 TBO, or it's designates, shall access reporting for the following:

a. Units in service, by type, billed customer, department.
b. Calls, by billed customer, pager number, department
c. Overcalls by billed customer, pager number, department
d. New sales, charges, or disconnects
e. Account Summary by sub-accounts
f. Zero-use devices

5.7.3 END-USER TRAINING

The Contractor provided web-based portal shall have self-paced web-based help tutorials covering all portal functionality.

In addition, the Contractor shall provide web-based training, for new VA managers or when significant changes to the web-based content have occurred. Contractor training shall be on a quarterly basis

DRAFT

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/EAOIT/OneVA/EAETA.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/docs_design_patterns.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63-2, VA Handbook 6500 Appendix F, “VA System Security Controls”, and VA IAM enterprise requirements for both direct and assertion based authentication. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of both Personal Identity Verification (PIV) and Common Access Card (CAC). Assertion authentication at a minimum must include Security Assertion Markup Language (SAML) token authentication and authentication/account binding based on trusted headers. Specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf), M-05-24 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf), M-11-11 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications. For applications, software, or hardware that cannot support PIV authentication, a Risk Based Decision must be approved by the Deputy Assistant Secretary for Information Security.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf) & (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in ac-

cordance with the USGv6: A Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm) and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html), shall be included in all IT infrastructures, application designs, application development, operational systems and subsystems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 (http://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2%200_2013.pdf).

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Internet Explorer 11, Office 2013, and Windows 8.1. However, Internet Explorer 11, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Internet Explorer 11, Office 2013, and Windows 8.1 individually as the VA standard, Internet Explorer 11, Office 2013, and Windows 8.1 will supersede Internet Explorer 9, Office 2010, and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Contractor shall support VA efforts in accordance with the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OI&T

Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

6.2 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	**Tier 1 / National Agency Check with Written Inquiries (NACI)** A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate / Tier 2	**Tier 2 / Moderate Background Investigation (MBI)** A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	**Tier 4 / Background Investigation (BI)** A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

	Position Sensitivity and Background Investigation Requirements		
Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	☒	☐	☐
5.2	☒	☐	☐
5.3	☒	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. The Contractor shall bear the expense of obtaining background investigations.
a. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff

Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

b. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
c. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints
    2) For Tier 2/Moderate or Tier 4/High Risk designation:
        a) OF-306
        b) VA Form 0710
        c) DVA Memorandum – Electronic Fingerprints
d. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
e. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
f. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
g. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).

h. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
i. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
j. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Performance Levels for Objectives associated with this effort.

Performance Objective	Performance Standard	Acceptable Performance Levels
A. Technical Needs	1. Shows understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Offers quality services/products	Satisfactory or higher
B. Project Milestones and	1. Quick response capability 2. Products completed, re-	Satisfactory or higher

Schedule	viewed, delivered in timely manner 3. Notifies customer in advance of potential problems	
C. Project Staffing	1. Currency of expertise 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Value Added	1. Provided valuable service to Government 2. Services/products delivered were of desired quality	Satisfactory or higher

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

FACILITY/RESOURCE PROVISIONS

Not Applicable

6.5 GOVERNMENT FURNISHED PROPERTY

Not Applicable

6.6 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

The Contractor(s) shall comply with all personnel security requirements included in this contract and local level organization security requirements described in each individual task order. Contractor Technicians will require escorts in VA facilities in accordance with Section 2.h (6) of VA Directive 0710 (see PWS section 6.1.1)

6.6.1 VA DIRECTIVE 0710 PERSONNEL SECURITY AND SUITABILITY PROGRAM

1. PURPOSE AND BACKGROUND. This directive describes the purpose, responsibilities, requirements, and procedures of VA's Personnel Security and Suitability Program, applicable to Federal applicants, appointees, employees, contractors and affiliates who

have access to departmental operations, facilities, information, or information technology systems.

a. The Personnel Security and Suitability Program has three main purposes:

(1) To provide a basis for determining a person's suitability to work for or on behalf of the government,

(2) To provide a basis for VA to determine whether a Federal employee should be granted a security clearance, and

(3) To implement certain Personal Identity Verification requirements of Federal Information Processing Standards (FIPS-201).

b. The Federal government mandates by law, executive order, Presidential Directives, regulations, and guidance that all applicants, appointees, employees, contractors, and others are suitable for employment or assignment to work for or on behalf of the Federal government.

c. Personnel Security and Suitability Programs were established in 1953 by Executive Order (EO) 10450, Security Requirements for Government Employment, as amended and enhanced in 1995 by EO 12968, Access to Classified Information, as amended. These orders set the standards for suitability and security clearance processes for the Federal government. The processes were reformed in 2008 by EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information.

d. EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, was issued June 30, 2008. This EO reformed the use of reciprocity across the Federal government to ensure cost-effective, timely, and efficient protection of national interests.

e. Office of Personnel Management (OPM) revised Title 5, Code of Federal Regulations (CFR), 731, Suitability in April 2008 and again in November 2008. These regulations are the framework for the Department of Veterans Affairs (VA's) Personnel Security and Suitability Program.

f. EO 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, was issued on January 16, 2009. This EO requires a reinvestigation on all individuals in positions of public trust to ensure that they remain suitable for continued employment.

g. The Intelligence Reform and Terrorism Prevention Action of 2004 (IRTPA), Public Law No. 108-458 (2004) (codified at 50 U.S.C. 435b) sets goals and timelines for granting clearances, ensuring reciprocity, and establishing an integrated database for completed background investigations.

2. POLICY

a. VA is required to establish criteria and procedures for making suitability determinations and taking suitability actions involving applicants for and appointees to covered positions. Suitability determinations are based on a person's character or conduct that may have an impact on the integrity or efficiency of the service. Determining suitability for Federal employment will be consistent with 5 Part CFR 731. Determining fitness for contractor employees will be based on criteria equivalent to that used for Federal employees. Determinations made under this category are distinct from determinations of eligibility for assignment to, or retention in, sensitive national security positions.

b. Some positions are also subject to sensitivity considerations relating to national security and access to classified information. Eligibility for access to classified information shall be granted in accordance with EO 12968, as amended. Eligibility determinations will be made using the standards set forth in the “Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.”
c. VA must implement policies and maintain records demonstrating that VA employs reasonable methods to ensure adherence to Office of Personnel Management (OPM) and other regulatory issuances in determining suitability for employment. Facilities are required to establish local policies and procedures to ensure that required background screenings are accomplished and documented.
d. This directive requires Administrations and staff offices to collaborate, participate, and recognize the shared, related, and interdependent responsibility to provide effective and efficient personnel security services to the department.
e. Designating Position Risk and Sensitivity Levels
(1) Agencies are required by 5 CFR, 731, Suitability, to designate the position risk level for all covered positions at Low, Moderate or High as determined by the position’s potential to adversely impact the efficiency and integrity of the service. High and Moderate Risk level positions are designated as Public Trust positions.
(2) All positions must also be given a sensitivity designation. National security positions are those that involve activities that are concerned with the protection of the United States from foreign aggression or espionage, the preservation of the Nation’s military strength, and the regular use of, or access to, classified information. The sensitivity designations are Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive. This designation is complimentary to the risk designation, and may have an effect on the position’s investigative requirement.
(3) All VA administrations and staff offices must use the Position Designation System and Automated Tool (PDAT) for designating position risk and sensitivity levels for all positions. The position designation process is used to determine the appropriate level of investigation for positions covered by 5 CFR, parts 731, Suitability, and 732, National Security Positions.
(4) The PDAT will be used by Contracting Officers and Contracting Officer Technical Representative to appropriately designate the statement of work or other written description of the assignment, with the proper risk or sensitivity level for the contract employees. Information Security Officers (ISO) should be consulted when access to VA information systems and data is involved to ensure appropriate risk levels are assigned for contractors.
f. Electronic Questionnaire for Investigations Processing (E-QIP). The use of E-QIP is mandated by the Office of Management and Budget (OMB) and OPM pursuant to the E-Government Act of 2002, P.L. 107-347. E-QIP allows applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to their employing agency for review and approval. E-QIP must be used for all investigative types for employees, contractors, affiliates, volunteers and other designated individuals who will need a background investigation.
g. Personal Identity Verification (PIV). FIPS 201-1 requires that at a minimum National Agency Check with Inquiries (NACI) be initiated prior to the issuance of a Personal Identity Verification (PIV) compliant card. Agencies can issue an electronically distin-

guishable identity credential on the basis of a completed FBI National Criminal History Check (fingerprint check) while the NACI is pending. OPM conducts Special Agreement Checks (SAC) which cover FBI criminal history. VA facilities must use electronic fingerprint equipment to submit SAC requests to OPM. All individuals who work for or at VA, whether they are paid or unpaid, with access to VA information or information systems, will be subject to background investigations pursuant to VA Directive 0735, “Personal Identity Verification (PIV) of Federal Employees and Contractors.”

h. Exemptions

(1) OPM has by regulation exempted the following positions from the investigative requirements of Executive Order (EO) 10450, Security Requirements for Government Employment, as amended.

(a) Low Risk/Non-sensitive positions that are temporary, intermittent, per diem, or seasonal not to exceed an aggregate of 180 days in either a single continuous appointment or series of appointments; and

(b) Positions filled by aliens outside the United States.

(2) Administrations and staff offices must conduct such checks as appropriate to ensure that the employment or retention of such individuals in these positions is consistent with the interests of national security.

(3) In accordance with National Institute of Standards and Technology (NIST) guidance, background screenings commensurate with the risk involved with the position will be conducted for any positions that require access to VA information systems.

(4) All individuals who work at or for VA, whether they are paid or unpaid, with access to VA information systems, will be subject to background screenings prior to being granted such access.

(5) By agreement with OPM, the investigative requirements as set forth in EO 10450 will not apply to the following categories of employees:

(a) Consultants or experts appointed to Low Risk/Non-sensitive positions for a period 1 year or less and not to be reappointed; and experts or consultants appointed for a period of more than 1 year or reappointed after a year with no break in service, provided the service does not exceed more than 30 days in any one calendar year.

(b) Physicians appointed under 38 U.S.C. 7406 to Low Risk/Non-sensitive positions as medical residents, provided they do not exceed 1 year of continuous service at a VA facility, regardless of the duration of the residency program.

(c) Purchase and hire employees appointed to Low Risk/Non-sensitive positions appointed for six months or less.

(6) Contract personnel assigned to Low Risk/Non-sensitive positions for 180 days or less under a single contract or a series of contracts.

(7) Any additional exemptions to the investigative requirements of EO 10450 must be approved by OPM, upon the request of the Secretary. Administrations and staff offices may submit requests for additional exemptions or modifications of existing exemptions through the Office of the Operations, Security, and Preparedness (OSP) for approval and submission to OPM.

i. Background Screening. VA requires that all personnel be subject to an appropriate background screening (Special Agreement Check (SAC)) prior to permitting access to VA information and information systems. This includes applicants, appointees, employ-

ees, contractors, affiliates and other individuals who require physical and/or logical access to VA information or information system

6.7 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: Microsoft (MS) Word, MS Excel, MS PowerPoint, and Adobe Postscript Data Format (PDF).

6.8 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Performance Levels for Objectives associated with this effort**.** Additional metrics may be required as defined in the individual TO.

Performance Objective	Performance Standard	Acceptable Performance Levels
Pager Service Plans(5.5)	The Contractor shall notify the VA COR, or his designate, and the VA National Service Desk (NSD) of any scheduled system outages at least 72 hours (including holiday and weekend hours) in advance of the planned outage. In case of any unforeseen outages, the VA-COR and the NSD shall be notified within four hours by both email and telephone call and kept up-to-date on the progress until service restoration. If the unscheduled outage is anticipated to be more than 24 hours, Contractor must provide an alternate plan for service coverage acceptable to VA.	99% uptime
Emergency Response time	Emergency repairs will be initiated within 2 hours of notification.	100% of all occurrences.

A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

6.9 GOVERNMENT FURNISHED INFORMATION

Government site plans, manuals, and drawings are applicable to this acquisition and will be provided to the Contractor as required for performance. All Government furnished information shall be returned at the completion of the contract.

6.10 GOVERNMENT FURNISHED PROPERTY

Not applicable.

ADDENDUM A

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance**.**

A2.1. VA Internet and Intranet Standards:

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed are published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards:

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.access-board.gov/sec508/standards.htm. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

_x_ § 1194.21 Software applications and operating systems
_x_ § 1194.22 Web-based intranet and internet information and applications
_x_ § 1194.23 Telecommunications products
_x_ § 1194.24 Video and multimedia products
_x_ § 1194.25 Self-contained, closed products
_x_ § 1194.26 Desktop and portable computers
_x_ § 1194.31 Functional Performance Criteria
_x_ § 1194.41 Information, Documentation, and Support

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and

164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:

a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
b. Controlled access to system and security software and documentation.
c. Recording, monitoring, and control of passwords and privileges.
d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

DRAFT

ADDENDUM B

APPLICABLE PARAGRAPHS TAILORED FROM: THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010

- GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

- ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or TO.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

- VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct onsite inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 calendar days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contrac-

tor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

- INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, VA Information Security Program). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, VA Privacy Impact Assessment.

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, VA Handbook 6500, Information Security Program and VA Handbook 6500.5, Incorporating Security and Privacy in System Development Lifecycle.

6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

c. Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

a. “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

b. “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods.

This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the severity of the incident.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

- INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, Certification and Accreditation and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, Electronic Media Sanitization upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

1) Vendor must accept the system without the drive;

2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

- SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

- LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results

in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:
a) date of occurrence;
b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
3) Number of individuals affected or potentially affected;
4) Names of individuals or groups affected or potentially affected;
5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
6) Amount of time the data has been out of VA control;
7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
8) Known misuses of data containing sensitive personal information, if any;
9) Assessment of the potential harm to the affected individuals;
10) Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and
11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

- SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

- TRAINING

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Contractor Rules of Behavior, Appendix D relating to access to VA information and information systems;
2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior training and annually complete required security training;
3) Successfully complete Privacy and HIPAA Training if Contractor will have access to PHI;
4) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
5) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access

b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

DRAFT

ADDENDUM C

VAMC Reno	975 Kirman Ave	Reno	NV	89502
VAMC Palo Alto	3801 Miranda Ave	Palo Alto	CA	94304
VAMC Long Beach	5901 E. 7th street	Long Beach	CA	90822
VAMC Las Vegas	6900 North Pecos Road	Las Vegas	NV	89086
VAMC Anchorage	1201 North Muldoon Road	Anchorage	AK	99504
VAMC Honolulu	459 Patterson Road	Honolulu	HI	96819
VAMC Puget Sound	1660 S. Columbian Way	Seattle	WA	98108
VAMC Los Angeles	11301 Wilshire Blvd	Los Angeles	CA	90073
VAMC San Diego	3350 La Jolla Village Drive	San Diego	CA	92161
VAMC Spokane	4815 N. Assembly street	Spokane	WA	99205
VAMC Loma Linda	11201 Benton street	Loma Linda	CA	92357
VAMC White City	8495 Crater Lake Hwy	White City	OR	97503
Tel Comm IT	650 E. Indian School Road	Phoenix	AZ	85012
VAMC Fresno	2615 E. Clinton Ave	Fresno	CA	93703
VAMC Portland	3710 SW U.S. Veteran Hospital Road	Portland	OR	97239
VAMC Roseburg	913 NW Garden Valley Blvd	Roseburg	OR	97471
VAMC Albuquerque	1501 San Pedro Drive, SE	Albuquerque	NM	87108
VAMC Tucson	3601 South 6th Avenue	Tucson	AZ	85723
VAMC San Francisco	4150 Clement Street	San Francisco	CA	94121
VAMC Denver	1055 Clermont Street	Denver	CO	80220
VAMC Phoenix	650 E. Indian School Road	Phoenix	AZ	85012
VA Northern CA Health Care System	10535 Hospital Way	Mather	CA	95655
VAMC Salt Lake City	500 Foothill Drive	Salt lake City	UT	84148
VAMC Fresno	2615 E. Clinton Ave	Fresno	CA	93703
VAMC Cheyenne	2360 E. Pershing Drive	Cheyenne	WY	82001
VAMC Prescott	500 North Highway 89	Prescott	AZ	86313

DRAFT